证　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：2002 11 13

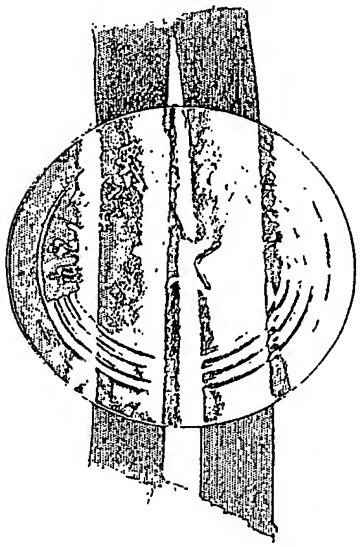
申　请　号：02 1 51984.6

申请类别：发明

发明创造名称：借助半导体存储装置实现数据安全存储和算法存储的方法

申　请　人：深圳市朗科科技有限公司

发明人或设计人：邓国顺；成晓华；向锋



中华人民共和国
国家知识产权局局长 王景川

2003 年 11 月 28 日

权 利 要 求 书

1、一种借助半导体存储装置实现数据安全存储的方法，包括有半导体存储装置，该半导体存储装置包括控制器模块以及分别与所述控制器模块电连接的通用接口模块和半导体存储介质模块，其特征在于：

所述数据安全存储方法包括以下步骤：

① 所述半导体存储介质模块分为至少两个逻辑存储空间；

② 所述逻辑存储空间中至少一个空间用于存储需要保护的数据；

③ 对所述半导体存储装置和/或所述至少一个逻辑存储空间设置并存储密码；

④ 在读/写操作前验证密码；

⑤ 向所述半导体存储装置写入所述需保护的数据时，所述控制器模块接收来自通用接口的数据，并把数据加密后存储在所述半导体存储介质模块中；

⑥ 从所述半导体存储装置读出所述需要保护的数据时，所述控制器模块把数据解密并通过通用接口将解密后的数据传送出去。

2、如权利要求 1 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：所述逻辑存储空间中至少一个空间用于存储算法，所述控制器模块根据来自通用接口的输入数据执行指定的算法，并把运算结果通过通用接口传送出去。

3、如权利要求 1 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：所述半导体存储介质模块可以是一种存储介质，或者是至少两种存储介质的组合。

4、如权利要求 1 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：对所述半导体存储装置和/或所述至少一个逻辑存储空间设置至少两级用户密码。

5、如权利要求 4 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：可以是对所有逻辑存储空间进行操作前验证用户密码，也可以是对存储需保护数据的逻辑存储空间进行操作前验证用户密码。

6、如权利要求 1、4 或 5 所述的借助半导体存储装置实现数据安全存储的方法，其特征在

于：设置数据库，并按照数据库的方式对所述需保护的数据进行存取和/或权限管理。

7、如权利要求 6 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：所述权限包括读取、写入、修改、删除和/或执行权限，各权限的具体含义分别是：

读取权限：只能够读取数据库中的记录数据；

写入权限：只能够向数据库中写入新的数据，但无法覆盖相同记录标题的记录数据；

修改权限：只能够向数据库中写入数据，同时能够覆盖相同记录标题的记录数据；

删除权限：够删除数据库中的记录或删除数据库；

执行权限：能够执行数据库中的记录代码，这是针对写入的数据是自定义算法或函数代码而设置的权限，一般记录数据指定执行权限无效。

8、如权利要求 1 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：所述逻辑存储空间中至少一个空间用于存储无需保护的数据。

9、如权利要求 1 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：对传输的数据和/或存储的数据进行防篡改识别。

10、 如权利要求 9 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：所述防篡改识别在数据发送或存储时包括以下步骤：

A、调用加密算法把原始数据进行变换获得变换值 X；

B、将原始数据和所述变换值 X 按照一定的格式打包成数据包；

C、发送或存储整个数据包；

在接收或读取数据时包括以下步骤：

A、按照上述同样的格式将数据包解包，获得原始数据和原始数据变换值 X；

B、调用上述相同的加密算法计算原始数据的变换值获得变换值 Y；

C、比较计算出的变换值 Y 与读出的变换值 X 是否相等；

D、如果比较结果相等，则数据没有被非法篡改，否则，数据已被篡改。

11、 如权利要求 1 或 9 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：在数据传输过程中，使用可随时改变的会话密钥对所述数据进行加密。

12、 如权利要求 11 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：所述采用可随时改变的会话密钥对数据进行加密的方法包括以下步骤：

A. 在数据传输过程开始时，发送端首先发送交换会话密钥命令，同时传入至少一个随机数；

B. 所述半导体存储装置收到交换会话密钥命令后，也随机生成至少一个随机数，并把收到的随机数和生成的随机数经过算法变换，产生会话密钥，然后把所述半导体存储装置生成的随机数返回给所述发送端；

C. 当所述发送端收到返回的随机数后，将接收到的随机数和发送端自己传入的随机数经过所述相同的算法变换，产生会话密钥。

13、 如权利要求 1 所述的借助半导体存储装置实现数据安全存储的方法，其特征在于：所述需要保护的数据包括但不限于文件、密码、密钥、帐号、数字证书、加密算法、自定义算法、用户信息和/或用户自定义数据。

14、 一种借助半导体存储装置实现算法存储的方法，包括有半导体存储装置，该半导体存储装置包括控制器模块以及分别与所述控制器模块电连接的通用接口模块和半导体存储介质模块，其特征在于：

所述算法存储方法包括以下步骤：

① 所述半导体存储介质模块分为至少两个逻辑存储空间；

② 所述逻辑存储空间中至少一个空间用于存储算法；

③ 所述控制器模块接收来自通用接口的输入数据；

④ 所述控制器模块根据输入数据执行指定的算法，并把运算结果通过通用接口传送出去。

15、 如权利要求 14 所述的借助半导体存储装置实现算法存储的方法，其特征在于：所述半导体存储介质模块只有一种存储介质，或者是至少两种存储介质的组合。

16、 如权利要求 14 所述的借助半导体存储装置实现算法存储的方法，其特征在于：所述算法是一个算法或多个算法。

17、 如权利要求 14 所述的借助半导体存储装置实现算法存储的方法，其特征在于：所述算法是所述半导体存储装置已内置的算法，或者是用户自定义的算法。

18、 如权利要求 14 所述的借助半导体存储装置实现算法存储的方法，其特征在于：对传输的数据和/或存储的数据进行防篡改识别。

19、 如权利要求 18 所述的借助半导体存储装置实现算法存储的方法，其特征在于：所述防篡改识别在数据发送或存储时包括以下步骤：

A、调用加密算法把原始数据进行变换获得变换值 X；

B、将原始数据和所述变换值 X 按照一定的格式打包成数据包；

C、发送或存储整个数据包；

在接收或读取数据时包括以下步骤：

A、按照上述同样的格式将数据包解包，获得原始数据和原始数据变换值 X；

B、调用上述相同的加密算法计算原始数据的变换值获得变换值 Y；

C、比较计算出的变换值 Y 与读出的变换值 X 是否相等；

D、如果比较结果相等，则数据没有被非法篡改，否则，数据已被篡改。

20、 如权利要求 14 或 18 所述的借助半导体存储装置实现算法存储的方法，其特征在于：在数据传输过程中，使用可随时改变的会话密钥对所述数据进行加密。

21、 如权利要求 20 所述的借助半导体存储装置实现算法存储的方法，其特征在于：所述采用可随时改变的会话密钥对数据进行加密的方法包括以下步骤：

A. 在数据传输过程开始时，发送端首先发送交换会话密钥命令，同时传入至少一个随机数；

B. 所述半导体存储装置收到交换会话密钥命令后，也随机生成至少一个随机数，并把收到的随机数和生成的随机数经过算法变换，产生会话密钥，然后把所述半导体存储装置生成的随机数返回给所述发送端；

C. 当所述发送端收到返回的随机数后，将接收到的随机数和发送端自己传入的随机数经过所述相同的算法变换，产生会话密钥。

说 明 书

借助半导体存储装置实现数据安全存储和算法存储的方法

技术领域 本发明涉及数据存储方法，尤其涉及一种借助半导体存储装置实现数据安全存储和算法存储的方法。

背景技术 在计算机技术飞速发展的今天，移动存储技术和移动存储产品也得到了快速发展。与磁存储软盘相比，无论从体积、容量、速度几方面均有了较大的突破。而且随着因特网的日益普及、电子商务的迅速发展，人们开始重视对所存储信息的保密处理，对用户认证的限制。如已公开的中国发明专利申请 01114762.8 “一种半导体存储装置”，提出了一种具有用户认证及数据加密与解密功能的半导体移动存储装置，对使用该半导体存储装置的用户加以身份认证，并对存入该半导体存储装置的信息进行加密保护，加密信息读出时再解密。但是，这种用户认证及数据加密技术是最简单、最低级的，很容易便被破解，已经不能满足人们对数据安全存储的需求。

随着 Internet 的发展，网上支付的新型电子交易支付手段开始迅速发展，成为各个商业银行、证券公司新的利润增长点和竞争焦点。因而，网络系统的安全问题，正变得日益突出，越来越受到人们的关注。人们不仅要防止网上黑客的随时攻击，更加担心自己的交易密码被他人盗取，以致在电子交易网络上的身份被他人非法冒用。各种信息钥匙产品随之产生，已有的信息钥匙，大多是内置唯一的用户密钥标识码和特殊算法程序的便携式电子产品，与计算机、信息电器等设备的通用外部接口相连，提供验证用户身份的功能，如中国实用新型专利 ZL01232435.3《信息钥匙》。信息钥匙是通过内置的简单用户密钥标识码验证虽然实现了用户身份认证，但存在以下不足：被破解的可能性很大：由于不支持用户自定义算法的写入，在使用上受到很大的限制，用于正版软件验证中时，其保护强度亦远远不能达到需求；忽视了用户对数据存储的需求。

发明内容 本发明所要解决的技术问题是改进现有加密技术的不足，提出一种借助半导体存储装置实现数据安全存储的方法，支持用户更高安全的移动数据存储，使合法用户数据被破解或泄密的难度极大地提高，从而极大地提高了用户存储数据的安全性。

本发明所解决的另一技术问题是提出一种借助半导体存储装置实现算法存储的方法，支持用户自定义算法的写入和内部执行，并返回运行结果，可广泛应用于身份认证、软件版权保护等信息安全领域。

本发明的技术问题需要通过采用以下技术方案来实现：设计一种借助半导体存储装置实现数据安全存储的方法，包括有半导体存储装置，该半导体存储装置包括控制器模块以及分别与所述控制器模块电连接的通用接口模块和半导体存储介质模块，所述数据安全存储方法包括以下步骤：

① 所述半导体存储介质模块分为至少两个逻辑存储空间；

② 所述逻辑存储空间中至少一个空间用于存储需要保护的数据；

③ 对所述半导体存储装置和/或所述至少一个逻辑存储空间设置并存储密码；

④ 在读/写操作前验证密码；

⑤ 向所述半导体存储装置写入所述需保护的数据时，所述控制器模块接收来自通用接口的数据，并把数据加密后存储在所述半导体存储介质模块中；

⑥ 从所述半导体存储装置读出所述需要保护的数据时，所述控制器模块把数据解密并通过通用接口将解密后的数据传送出去。

本发明的技术问题还需要通过采用以下技术方案来实现：设计一种借助半导体存储装置实现算法存储的方法，包括有半导体存储装置，该半导体存储装置包括控制器模块以及分别与所述控制器模块电连接的通用接口模块和半导体存储介质模块，所述算法存储方法包括以下步骤：

① 所述半导体存储介质模块分为至少两个逻辑存储空间；

② 所述逻辑存储空间中至少一个空间用于存储算法；

③ 所述控制器模块接收来自通用接口的输入数据；

④ 所述控制器模块根据输入数据执行指定的算法，并把运算结果通过通用接口传送出去。

本发明借助半导体存储装置实现数据安全存储和算法存储的方法，还设计有双重密码管理，设置多重管理权限，以及数据库控制、随机加密和防篡改技术等。

本发明在提供用户数据移动存储的同时，采用高级安全存储技术，同时，本发明提供开放式的应用接口，支持用户自定义算法的写入和调用。与现有技术相比，本发明具有以

下技术效果：能同时实现普通数据存储、需保密数据和/或算法存储的功能；数据存储的安全性大大提高，能广泛适用于信息安全领域，如软件版权保护、网上银行、网上购物、社保医保、个人身份和网上身份识别、电子交易、数字证书、工商管理以及税务管理等。

附图说明

图 1 是本发明借助半导体存储装置实现数据安全存储和算法存储的方法的实施原理图；

图 2 是实现本发明数据安全存储和算法存储方法的半导体存储装置的结构原理图；

图 3 是本发明数据安全存储的方法在数据发送或存储时数据防篡改实现流程图；

图 4 是本发明数据安全存储的方法在数据接收或读取时数据防篡改实现流程图；

图 5 是本发明数据安全存储的方法中数据传输采用会话密钥加密的流程图；

图 6 是本发明数据安全存储和算法存储的方法用于软件版权保护时的软件执行流程图；

图 7 是本发明数据安全存储和算法存储的方法用于软件版权保护时的用户自定义算法调用流程图；

图 8 是本发明数据安全存储和算法存储的方法用于软件版权保护时的多模块管理实现流程图；

图 9 是图 2 所示半导体存储装置采用 USB 接口和快闪存储器的结构原理图；

图 10-A、B、C 是图 9 中采用 USB 接口和快闪存储器的半导体存储装置电路原理图。

具体实施方式 下面结合附图对本发明的最佳实施例作进一步详细说明：

如图 1 所示，本发明借助半导体存储装置实现数据安全存储和算法存储的方法，通过本发明提供的开发接口连接到与操作系统相关的半导体存储装置驱动程序，然后通过半导体存储装置的驱动程序经由通用接口与该接口上的半导体存储装置交互作用，实现各种安全应用。

本发明借助半导体存储装置实现数据安全存储的方法，如图 2 所示，包括有半导体存储装置，该半导体存储装置包括控制器模块 1 以及分别与所述控制器模块 1 电连接的通用接口模块 2 和半导体存储介质模块 3，所述数据安全存储方法包括以下步骤：

① 所述半导体存储介质模块 3 分为至少两个逻辑存储空间；

② 所述逻辑存储空间中至少一个空间用于存储需要保护的数据；

③ 对所述半导体存储装置和/或所述至少一个逻辑存储空间设置并存储密码；

④ 在读/写操作前验证密码；

⑤ 向所述半导体存储装置写入所述需保护的数据时，所述控制器模块 1 接收来自通用接口 2 的数据，并把数据加密后存储在所述半导体存储介质模块 3 中；

⑥ 从所述半导体存储装置读出所述需要保护的数据时，所述控制器模块 1 把数据解密并通过通用接口 2 将解密后的数据传送出去。

本发明借助半导体存储装置实现算法存储的方法，如图 2 所示，包括有半导体存储装置，该半导体存储装置包括控制器模块 1 以及分别与所述控制器模块 1 电连接的通用接口模块 2 和半导体存储介质模块 3，所述算法存储方法包括以下步骤：

① 所述半导体存储介质模块 3 分为至少两个逻辑存储空间；

② 所述逻辑存储空间中至少一个空间用于存储算法；

③ 所述控制器模块 1 接收来自通用接口 2 的输入数据；

④ 所述控制器模块 1 根据输入数据执行指定的算法，并把运算结果通过通用接口 2 传送出去。

本发明所述的半导体存储装置参见中国专利 ZL99117225.6“用于数据处理系统的快闪电子式外存储方法及其装置”，该专利公开了一种利用快闪存储器（Flash Memory）作为存储介质的半导体存储装置，基于 USB、IEEE1394 等通用接口实现大容量数据的移动存储，其应用已是越来越得到普及。

所述通用接口 2，是所述半导体存储装置与数据处理系统连接的接口，也是实现本发明各种安全应用的通信接口。该通用接口可以是有线通用接口或者是无线通用接口，接口类型包括串口、并口、USB 接口、IEEE1394 接口、蓝牙（Bluetooth）接口、IrDA 红外接口、HomeRF 接口、IEEE802.11a 接口或 IEEE802.11b。

所述半导体存储介质模块 3 至少分为两个逻辑存储空间，其中至少一个逻辑存储空间用于存储需要保护的数据，至少一个逻辑存储空间用于存储无需保护的数据。所述半导体存储介质模块 3 可以是一种存储介质，也可以是至少两种存储介质的组合。所述半导体存

储介质包括但不限于快闪存储器（Flash Memory）、DRAM、EEPROM、SRAM、FRAM、MRAM 或者是 Millipede，可以采用一块或多块半导体芯片。所述半导体存储介质模块 3 的逻辑存储空间可以设置在一种存储介质上，也可以设置在至少两种存储介质上。所述至少一个逻辑存储空间中存储的需保护的数据包括但不限于文件、密码、密钥、帐号、数字证书、加密算法、自定义算法、用户信息和/或用户自定义数据。

所述半导体存储装置通过与数据处理系统连接从通用接口获得电源供应；当所述通用接口 2 是无线通用接口时，该存储装置可以自带电源或从外部电源获取电源供应。因现今该类半导体存储装置有关电源供应的文献已较多，在此作过多不再赘述。

所述控制器模块1是所述半导体存储装置的核心控制模块，所述控制器模块1中内置有固化软件（即Firmware），该固化软件主要功能在于：

a) 通过通用接口控制所述半导体存储装置与数据处理系统之间的数据通信或数据读写，实现用户的大容量数据移动存储功能；
b) 接受来自数据处理系统的控制信息和/或操作请求，并根据所述的控制信息和/或操作请求执行相应操作；
c) 执行已内置的或用户自定义写入的各种算法，并返回运算结果；
d) 调用预先定义的数据加密解密系统，对用户存储的数据进行数据加密或解密，实现用户数据的安全存储；

所述控制器模块 1 中的固化软件还提供了开放的应用开发接口，用户可以通过应用开发接口的动态链接，在此基础上开发各种安全加密、身份识别、版权保护等更为强大的应用；所述控制器模块 1 中的固化软件还为用户自定义算法和函数提供了统一的输入输出参数定义，使用户定义强大的算法也成为可能。

如图 9 所示，所述半导体存储装置采用 USB 接口和快闪存储器（Flash Memory），包括控制器模块 1、快闪存储器模块 31 和 USB 接口模块 21，所述快闪存储器 31 和 USB 接口 21 分别和控制器模块 1 建立电连接。所述半导体存储装置还包括电源模块 5、写保护开关 6 和状态指示模块 7。

图 10-A、B、C 是所述半导体存储装置的电路原理图，图 10-A 中，所述控制器模块 1

采用 Hitachi 公司的 H8S2215 MCU 作为主控制器，H8S2215 芯片提供了 64K ROM、8K RAM、16Bit 级的时钟频率，运行速度快；S1 器件为写保护开关，当 S1 拨至与 FWP-信号连接的引脚处于“0”电平时，所述半导体存储装置处于写保护状态，可读不可写，反之处于正常可读可写状态；所述状态指示采用 LED 指示灯 D1，GL-是指示灯控制信号，当对所述半导体存储装置进行读写、删除等操作时，D1 闪烁，否则常亮。所述的快闪存储器模块 31，如图 10-B 所示，包括 U14、U15 两块 NAND 型快闪存储器芯片，其中 D0~D7 为数据总线，控制信号包括 FALE、FCLE、FWR-、FRD-、FCE1-、FCE2-，并分别与 H8S2215 芯片的相应端连接；状态信号包括 FWP-、FRB-，分别与 H8S2215 芯片的相应端连接。如图 10-C 所示，通用接口模块 2 采用 USB 接口，且所述半导体存储装置从数据处理系统 USB 总线取得供电源，其中 U1 及其外围元件组成整个系统的供电电路。

本发明借助半导体存储装置实现数据安全存储的方法进一步说明如下：

本发明所述借助半导体存储装置实现数据安全存储的方法，支持需保护数据的多级密码多级权限管理设置。所述需保护的数据，存储在所述半导体存储装置的至少一个逻辑存储空间里，包括但不限于文件、密码、密钥、帐号、数字证书、加密算法、自定义算法、用户信息和/或用户自定义数据。所述需保护的数据经过特定的加密算法加密，如不能获得正确的加密密钥，将无法正确有效地读取该数据。

本发明所述数据安全存储方法，对所述半导体存储装置设置至少两级用户密码，即高级管理员密码和普通用户密码；为了实现更强大的数据存储管理，本发明也可以设置多级用户密码，实现多用户管理。本发明所述数据安全存储方法，也可以只对所述半导体存储介质模块的一个逻辑存储空间或几个逻辑存储空间设置两级密码。

为了保护数据的安全性，在对所述半导体存储装置进行读/写操作前，需要验证用户密码。所述验证用户密码可以是对所有逻辑存储空间进行操作前验证用户密码；也可以是仅对存储需保护数据的逻辑存储空间进行操作前验证用户密码，任何用户都可以对存储无需保护数据的逻辑存储空间进行任何操作。所述验证用户密码，可以是在所述半导体存储装置上电初始化后一次性的验证用户密码，以后直至所述半导体存储装置拔除前对所述半导体存储装置的任何操作都无需再验证用户密码；也可以是对所述半导体存储装置的每一次

读/写操作前都必须验证用户密码；还可以是在对所述半导体存储装置的读/写操作前间隔的或者随机的验证用户密码。

本发明所述借助半导体存储装置实现数据安全存储的方法，为实现数据的分类存储，引入数据库数据存储设计理念，设置数据库，并按照数据库的方式对所述需保护的数据进行存取和/或权限管理。

为了分类组织数据，高级管理员和普通用户都可以创建自己的数据库，并在创建时指定数据库的记录是否需要加密；同时，在创建数据库时还可以指定数据库的访问权限。

数据库创建时可以指定读取、写入、修改、删除和执行权限，各权限的具体含义如下：

读取权限：只能够读取数据库中的记录数据；

写入权限：只能够向数据库中写入新的数据，但无法覆盖相同记录标题的记录数据。

修改权限：只能够向数据库中写入数据，同时能够覆盖相同记录标题的记录数据。

删除权限：够删除数据库中的记录或删除数据库；

执行权限：能够执行数据库中的记录代码，这是针对写入的数据是自定义算法或函数代码而设置的权限，一般记录数据指定执行权限无效。

为了控制需保护数据的安全访问，对于高级管理员创建的数据库，普通用户只拥有高级管理员为其设置的访问权限；而且，普通用户不能创建高级管理员已经创建的数据库。

本发明所述数据安全存储方法，向所述半导体存储装置写入所述需保护的数据时，所述控制器模块 1 接收来自通用接口 2 的所述需保护的数据，然后经过加密后存储在所述半导体存储介质模块 3 的至少一个逻辑存储空间里的。所述被保护数据可以采用普通用户密码或普通用户密码经过加密算法变换后的数据作为密钥加密后存储。因此，高级管理员要正确访问所述需保护的数据，必须验证普通用户密码，这样可以保证普通用户写入的数据的保密性。同时，高级管理员写入需要保护的数据时，也必须先验证普通用户密码，才能获得加密密钥对数据库进行加密，否则写入的数据只能是不加密的。从所述半导体存储装置读出所述需保护的数据时，所述控制器模块 1 根据验证普通用户密码获得的加密密钥解密所述需保护的数据，并通过通用接口 2 将解密后的数据传送出去。

高级管理员对所有数据库拥有最高控制权。对于普通用户创建的数据库，即使不验证普通用户密码，高级管理员也可以对其进行读取、写入、修改、删除和执行，但是因为没有取得加密密钥，读取、写入、修改的数据将无法正确加/解密，导致数据无法正确读取。

在信息安全领域中，某些不法人士获得非法使用的常用手段是跟踪数据的变化，找到规律后修改运行代码。为了保护传输中的数据和/或存储的数据不被非法篡改，本发明数据安全存储方法具有识别数据是否被篡改的设计。根据数据安全性的要求，可以对所有所述需保护数据进行防篡改识别，也可以仅对传输的和/或存储的某些关键数据进行防篡改识别。对传输的数据和/或存储的数据进行防篡改识别，如图 3 和图 4 所示，具体实现如下：

在数据发送或存储时，如图 3 所示，包括以下步骤：

A、调用加密算法把原始数据进行变换获得变换值 X；

B、将原始数据和所述变换值 X 按照一定的格式打包成数据包；

C、发送或存储整个数据包；

在接收或读取数据时，如图 4 所示，包括以下步骤：

A、按照上述同样的格式将数据包解包，获得原始数据和原始数据变换值 X；

B、调用上述相同的加密算法计算原始数据的变换值获得变换值 Y；

C、比较计算出的变换值 Y 与读出的变换值 X 是否相等；

D、如果比较结果相等，则数据没有被非法篡改，否则，数据已被篡改。

本发明所述数据安全存储的方法，为防止数据在传输过程中被截取，除了采用防篡改设计外，在所述半导体存储装置与数据处理系统交换数据的过程中采用可随时改变的会话密钥对数据加密，如图 5 所示，具体实现如下：

A. 在数据传输过程开始时，发送端首先发送交换会话密钥命令，同时传入至少一个随机数；

B. 所述半导体存储装置收到交换会话密钥命令后，也随机生成至少一个随机数，并把收到的随机数和生成的随机数经过算法变换，产生会话密钥，然后把所述半导体存储装置生成的随机数返回给所述发送端；

C. 当所述发送端收到返回的随机数后，将接收到的随机数和发送端自己传入的随机数经过所述相同的算法变换，产生会话密钥。

所述会话密钥即作为数据处理系统和所述半导体存装置传输需保护数据时的加/解密密

钥。所述会话密钥可以随时因发送端发送改变会话密钥的请求而改变，从而保证了需保护数据传输的安全性。

本发明借助半导体存储装置实现算法存储的方法进一步说明如下：

本发明借助半导体存储装置实现算法存储的方法，所述半导体存储介质模块 3 分为至少两个逻辑存储空间，其中至少一个逻辑存储空间用于存储算法，所述控制器模块 1 根据来自通用接口 2 的输入数据执行指定的算法，并把运行结果通过通用接口 2 传送出去。

本发明算法存储的方法，所述算法存储在所述半导体存储介质模块 3 的至少一个逻辑存储空间里，可以采用本发明所述的数据安全存储方法存储，设置至少两级用户密码和多级权限管理，采用防篡改和会话密钥加密设计。所述存储的算法可以是一个或多个算法；可以是所述半导体存储装置已内置的算法，也可以用户通过应用接口写入的自定义算法。

本发明的算法存储方法，所述控制器模块 1 能根据来自通用接口 2 的输入数据执行指定的算法，并把运行结果通过通用接口 2 传送出去。所述控制器模块 1 把至少一个算法从半导体存储介质模块 3 中读出并加载到控制器模块 1 中，然后根据从通用接口 2 接收到的算法调用参数选择至少一个算法并在控制器内部执行该算法，然后将运算结果通过通用接口 2 返回。或者，所述控制器模块 1 根据从通用接口 2 接收到的算法调用参数选择至少一个算法，然后把该算法从半导体存储介质模块 3 中读出并加载到控制器模块 1 中，然后在控制器内部执行该算法并将运算结果通过通用接口 2 返回。

下面以软件版权保护作为实施例对本发明所述借助半导体存储装置实现数据安全存储和算法存储的方法进行更进一步的说明：

本发明所述数据安全存储和算法存储的方法，提供用户开放式的应用接口，支持用户自定义算法的写入和调用。本发明数据安全存储和算法存储的方法为实现软件版权保护提供给软件开发商的常用开发接口如下：

1） 初始化所述半导体存储装置：DWORD NetacOD_Init(OD_INFO *odInfo);

2） 退出所述半导体存储装置：DWORD NetacOD_Exit( );

3） 验证普通用户密码：

DWORD NetacOD_AuthUserPwd(unsigned char pwd[17], int odIndex = 1);

4） 验证高级管理员密码：

DWORD NetacOD_AuthAdminPwd(unsigned char pwd[17], int odIndex = 1);

5） 创建用户数据库：DWORD NetacOD_CreateUserDB(unsigned char DBType, unsigned char bEncrypt, unsigned char bAccess, unsigned char *DBId, int odIndex = 1);

6） 打开数据库：DWORD NetacOD_OpenUserDB(unsigned char DBType, unsigned char bAccess, unsigned char *DBId, int odIndex = 1);

7） 删除数据库：

DWORD NetacOD_DeleteUserDB(unsigned char DBID,int odIndex = 1);

8） 关闭数据库：

DWORD NetacOD_CloseUserDB(unsigned char DBID,int odIndex = 1);

9） 向数据库写入用户数据：DWORD NetacOD_WriteUserData(unsigned char DBID, unsigned char dataID[9], unsigned char *data, unsigned short dataLen, int odIndex = 1);

10） 删除数据库中某条记录：DWORD NetacOD_DeleteUserData(unsigned char DBID, unsigned char dataID[9], bool bIsIndexNo = FALSE, int odIndex = 1);

11） 读取数据库中制定标识记录：DWORD NetacOD_ReadUserData(unsigned char DBID, unsigned char dataID[9], unsigned char *data, unsigned short *dataLen, bool bIsIndexNo = FALSE, int odIndex = 1);

12） 写入软件模块数据：DWORD NetacOD_WriteModuleData(unsigned char moduleID, unsigned char moduleAttr, unsigned short moduleUseCounter, unsigned short moduleUserCounter=1, int odIndex = 1);

13） 读出软件模块数据：DWORD NetacOD_ReadModuleData(MODULE_INFO *moduleInfo, int odIndex = 1);

14） 递减软件某模块设定的使用次数：

DWORD NetacOD_DecreaseCounter(unsigned char moduleID,int odIndex = 1);

15） 写入自定义算法和函数：DWORD NetacOD_WriteFunction(unsigned char functionName[9], unsigned char* functionData, unsigned short functionDataLen, int odIndex = 1);

16） 调用写入的自定义算法和函数：DWORD NetacOD_CallFunction(IN_PARAM*

functionInParameter, OUT_PARAM* functionOutParameter, int odIndex = 1);

17）调用哈希算法：DWORD NetacOD_Hash(IN PHASH_PROPERTY pHashProperty, IN PBYTE pInBuffer, IN WORD wInBufferLen, IN OUT PBYTE pOutBuffer, IN OUT PWORD pOutBufferLen);

18）加密：DWORD NetacOD_Encrypt(IN WORD wBitLen, IN BYTE bAlgId, IN PBYTE pKey, IN PBYTE pInBuffer, IN WORD wInBufferLen, IN OUT PBYTE pOutBuffer, IN OUT PWORD pOutBufferLen);

19）解密：DWORD NetacOD_Decrypt (IN WORD wBitLen, IN BYTE bAlgId, IN PBYTE pKey, IN PBYTE pInBuffer, IN WORD wInBufferLen, IN OUT PBYTE pOutBuffer, IN OUT PWORD pOutBufferLen);

20）生成密钥：DWORD NetacOD_GenKey(IN PKEY_ATTRpkeyAttr, IN PKEY_SEED pKeySeed, IN OUT PBYTE pKeyBuffer);

21）更改会话密钥：DWORD NetacOD_ChangeSessionKey();

基于上述接口，软件开发商可编写高强度的自定义算法和函数作为正版软件保护的调用算法，然后编译成所述半导体存储装置专用的执行代码，采用本发明的数据安全存储方法加密后写入到所述半导体存储装置中，实现源代码级的数据安全保护。

为了防止所述半导体存储装置在所述正版软件通过正版验证后被拔出或被切断通信（如蓝牙接口的连接），使一些不法人士跟踪或破解所述正版软件的加密算法，从而使所述正版软件有可能被非法使用，所述正版软件在运行过程中，以随机的时间间隔调用存储在所述半导体存储装置内的自定义特定算法。如图 6 和图 7 所示，具体实现如下：

A、所述正版软件通过简单的 API 函数调用向所述半导体存储装置的驱动程序发出“算法调用指令”，驱动程序自动将“算法调用指令”通过通用接口传递给所述半导体存储装置控制器模块 1；

B、所述半导体存储装置验证传入的算法调用参数是否被篡改，若被篡改，则退出程序运行；

C、所述半导体存储装置验证用户访问权限，若用户无自定义算法数据库的访问权限，则返回权限错误码；

D、所述半导体存储装置验证调用的模块是否允许运行，若用户无该模块使用权限，则返回模块错误码；

E、所述半导体存储装置对自定义算法进行解密，若解密读取不成功，则返回算法错误码；

F、所述半导体存储装置通过控制器模块 1 加载所述用户写入的算法代码到指定地址并运行，然后通过通用接口返回成功运行通知给所述半导体存储装置的驱动程序；

G、所述驱动程序将成功运行通知返回给所述软件中的 API 函数调用；

H、当所述正版软件收到算法调用成功运行通知时，发送“查询命令”给所述半导体存储装置，所述半导体存储装置返回当前用户自定义算法产生的应答结果；

I、所述被保护软件根据返回的应答结果进行相应的处理。所述软件根据调用的算法的不同，将两种不同的处理：在需要比较应答结果的情况下，若所述半导体存储装置返回的应答结果与所述软件的预期结果相同，程序正常运行，否则程序退出；在不需比较应答结果的情况下，若所述半导体存储装置返回的应答结果是正确的，程序正常运行，否则程序获得错误结果，可能导致异常产生和程序退出。

上述自定义算法的调用过程在软件运行的整个过程中以随机的时间间隔不断循环，若用户拔出所述半导体存储装置或切断所述半导体存储装置和所述软件之间的通信，所述软件检测不到半导体存储装置，自定义算法调用无法进行，则所述软件程序退出运行。本发明调用的算法可以是已内置的某种算法函数，也可以是用户通过开发接口写入的自定义算法，还可以是软件程序的一部分，经过编译后写入所述半导体存储装置。

根据本发明数据安全存储方法中的两级密码多级权限管理，作为高级管理员的软件开发商可以事先在所述半导体存储装置内写入调用算法、软件模块管理参数等设置信息，并分配给使用普通用户密码的软件使用者相应的访问权限。在安装和/或执行软件时，所述半导体存储装置验证普通用户密码，然后根据软件开发商事先的设置给普通用户分配相应的访问权限，从而控制了终端软件用户对所述半导体存储装置的操作，实现了对所述软件的使用控制。

大型的软件一般都分为很多模块，各模块可以单独或组合使用以实现不同的功能。根据本发明数据安全存储的方法，软件开发商可以在所述半导体存储装置内写入模块权限管理数据库，通过模块参数设置来满足不同用户的需求。

软件开发商在其为用户开发的应用程序中，设置模块调用自定义算法的参数，并在所述半导体存储装置内写入模块权限管理数据库，随机产生对应可使用模块的模块令牌号。在应用软件中设置模块调用接口调用自定义算法时，需要传入经模块令牌号签名后的算法调用参数进行验证，如果此模块不允许运行，则自定义算法调用失败，用户将不能使用该模块功能。为了防止用户通过更改算法调用参数来获得软件模某模块的非法使用，所述算法调用参数在传输过程中采用了本发明数据安全存储方法中的防篡改设计。如图 8 所示，实现模块管理的具体步骤如下：

A. 调用前，所述正版软件先在本地调用签名函数获得签名；

B. 用签名数据登录所述半导体存储装置内的模块权限管理数据库，获得该模块的令牌号；

C. 用模块令牌号签名调用算法的参数，调用存储在所述半导体存储装置内的自定义算法；

D. 所述半导体存储装置根据模块权限设置验证输入的算法调用参数签名是否正确，即判算法调用参数是否被篡改，如果正确则算法调用正常进行，允许所述正版软件该模块的执行，否则调用将失败，拒绝所述正版软件该模块的执行。

在调用所述半导体存储装置的自定义算法时，设置允许递减标志，则可通过接口递减所述正版软件某模块或该正版软件的使用次数和使用人数，如用户没有在限定次数或人数内成功登陆，则无法成功调用所述半导体存储装置内的自定义算法，即无法运行所述正版软件的某模块或该软件。同时，为防止数据在传输过程中被截取，除了采用防篡改设计外，还可以采用本发明数据安全存储方法中的随时可改变的会话密钥加密技术对数据进行加密，进一步增强数据传输过程中的安全性。

本发明借助半导体存储装置实现数据安全存储和算法存储的方法，还可以广泛应用于网上银行、电子交易等众多信息安全领域。在网上银行进行交易，人们最担心的就是怕自己的交易密码被他人盗取，从而在网络上的身份被他人非法冒用。根据本发明的数据安全存储方法，用户的个人资料、私钥、数字证书等信息安全存储在所述半导体存储装置的半导体存储介质模块中，并通过控制器模块执行内置的算法来实现身份认证的功能。只有该半导体存储装置的使用者本人才能携带和唯一的使用该标明其身份的装置，在该装置内部完成数字签名等私钥运算，从而杜绝任何信息的泄漏。利用本发明的数据安全存储和算法

存储方法，借助所述半导体存储装置，只要在有计算机且能够连接互联网的地方，即使是在消费者家里或公共网吧里，也能够进行网上安全可靠的交易和支付。

说明书附图

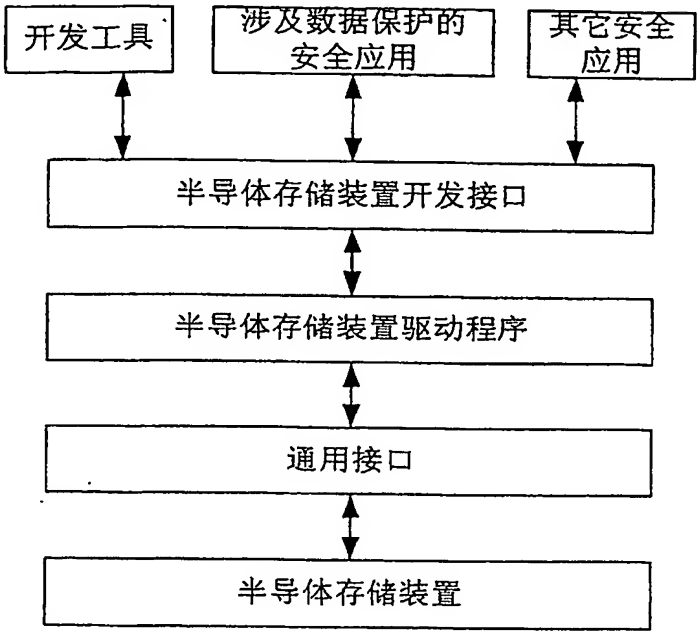

开发工具
涉及数据保护的安全应用
其它安全应用
半导体存储装置开发接口
半导体存储装置驱动程序
通用接口
半导体存储装置

图 1

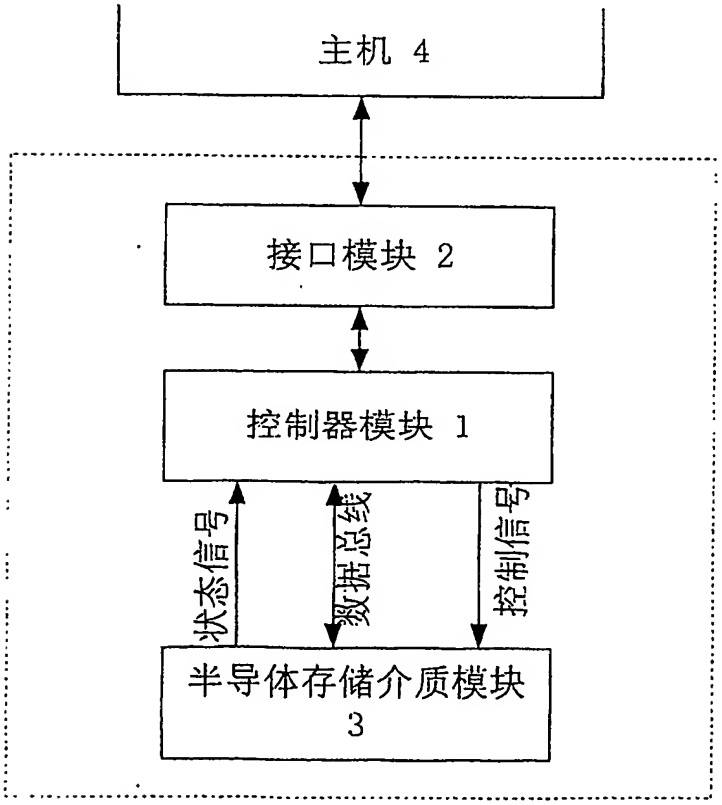

主机 4
接口模块 2
控制器模块 1
状态信号
数据总线
控制信号
半导体存储介质模块 3

图 2

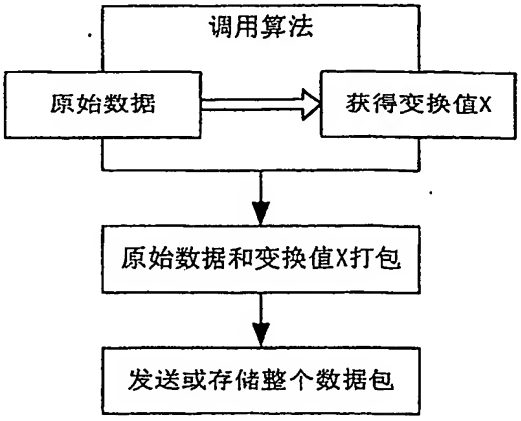

调用算法
原始数据
获得变换值X
原始数据和变换值X打包
发送或存储整个数据包

图 3

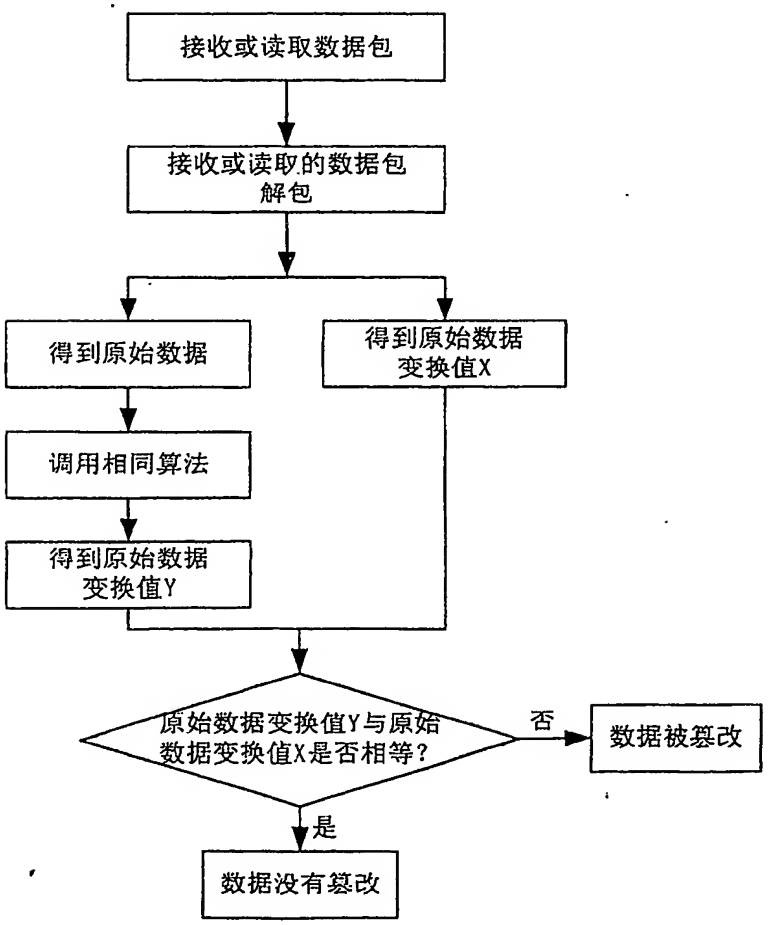

接收或读取数据包
接收或读取的数据包
解包
得到原始数据
得到原始数据
变换值X
调用相同算法
得到原始数据
变换值Y
原始数据变换值Y与原始
数据变换值X是否相等?
否
数据被篡改
是
数据没有篡改

图 4

说明书附图

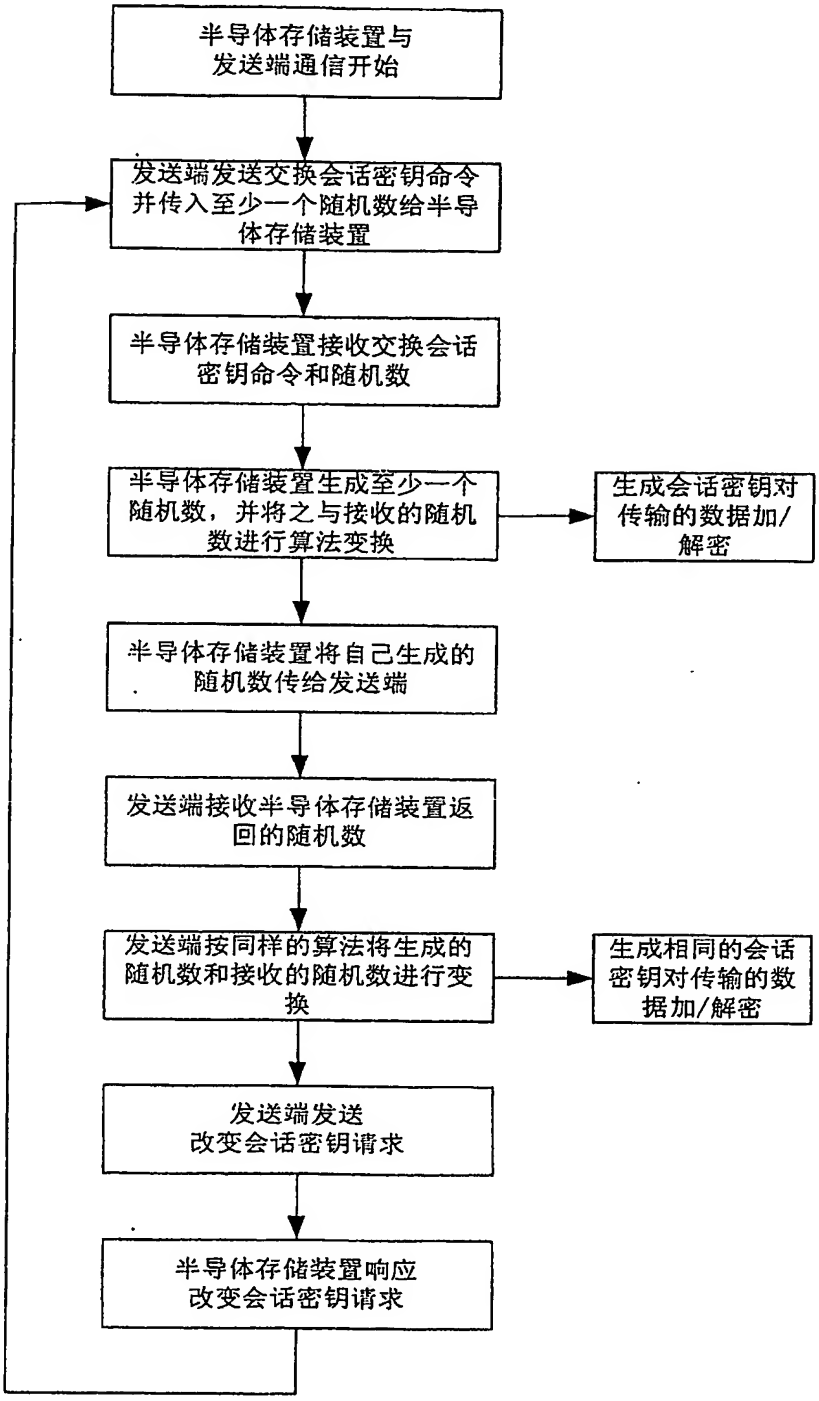

半导体存储装置与发送端通信开始
发送端发送交换会话密钥命令并传入至少一个随机数给半导体存储装置
半导体存储装置接收交换会话密钥命令和随机数
半导体存储装置生成至少一个随机数，并将之与接收的随机数进行算法变换
生成会话密钥对传输的数据加/解密
半导体存储装置将自己生成的随机数传给发送端
发送端接收半导体存储装置返回的随机数
发送端按同样的算法将生成的随机数和接收的随机数进行变换
生成相同的会话密钥对传输的数据加/解密
发送端发送改变会话密钥请求
半导体存储装置响应改变会话密钥请求

图 5

说明书附图

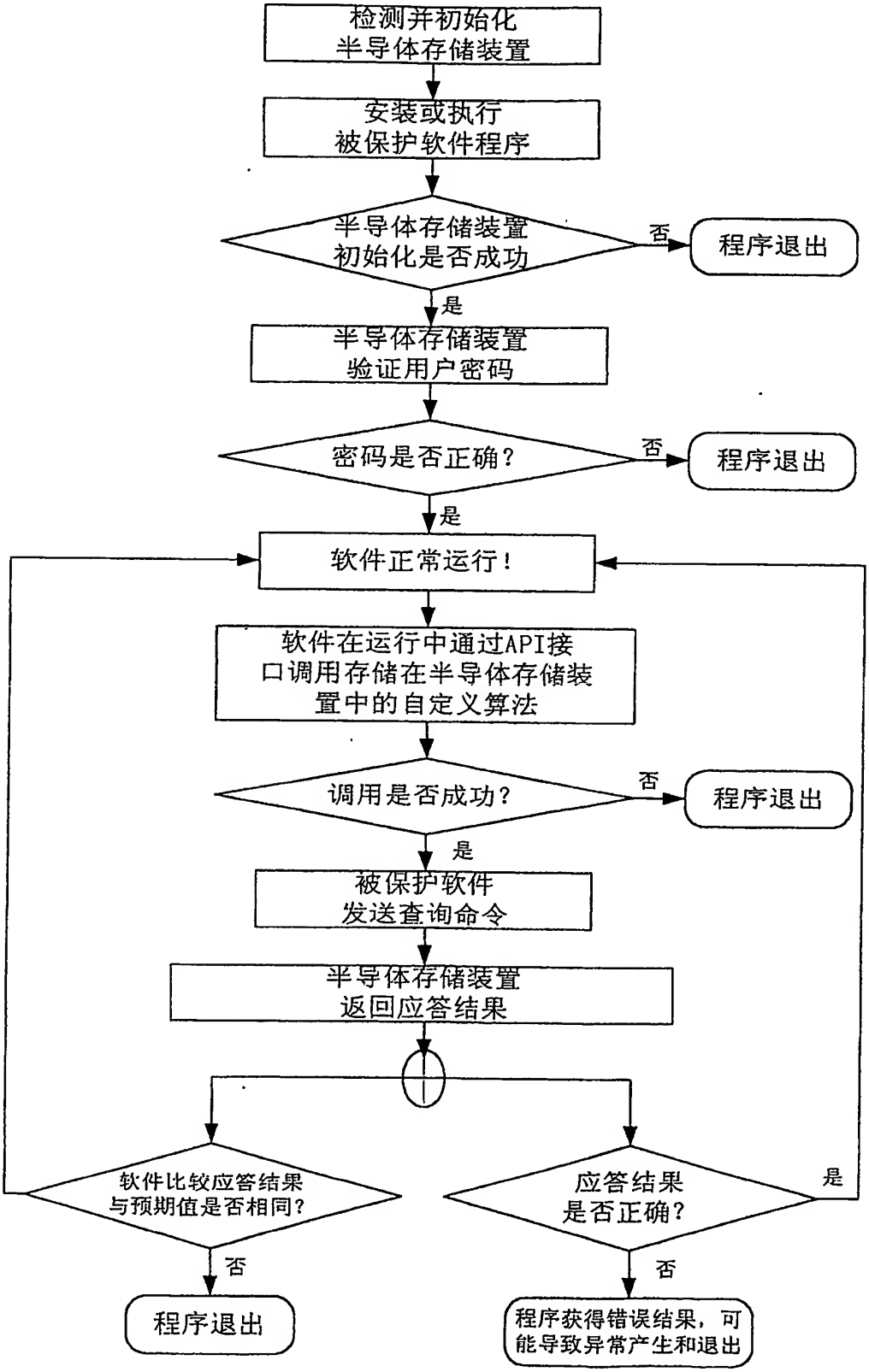

检测并初始化
半导体存储装置
安装或执行
被保护软件程序
半导体存储装置
初始化是否成功
否
程序退出
是
半导体存储装置
验证用户密码
密码是否正确？
否
程序退出
是
软件正常运行！
软件在运行中通过API接
口调用存储在半导体存储装
置中的自定义算法
调用是否成功？
否
程序退出
是
被保护软件
发送查询命令
半导体存储装置
返回应答结果
软件比较应答结果
与预期值是否相同？
否
程序退出
应答结果
是否正确？
是
否
程序获得错误结果，可
能导致异常产生和退出

图 6

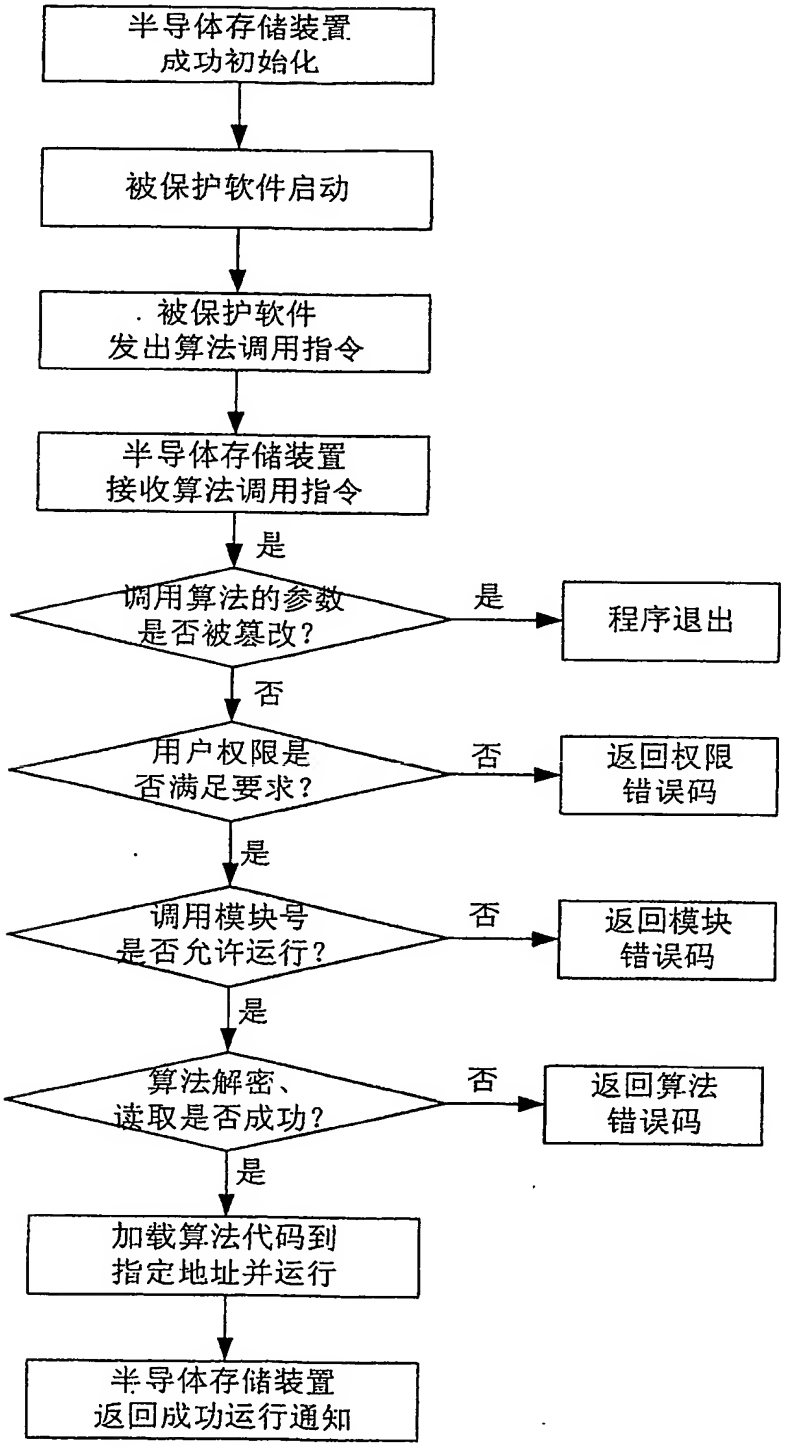

半导体存储装置
成功初始化
被保护软件启动
被保护软件
发出算法调用指令
半导体存储装置
接收算法调用指令
是
调用算法的参数
是否被篡改？
是
程序退出
否
用户权限是
否满足要求？
否
返回权限
错误码
是
调用模块号
是否允许运行？
否
返回模块
错误码
是
算法解密、
读取是否成功？
否
返回算法
错误码
是
加载算法代码到
指定地址并运行
半导体存储装置
返回成功运行通知

图 7

说明书附图

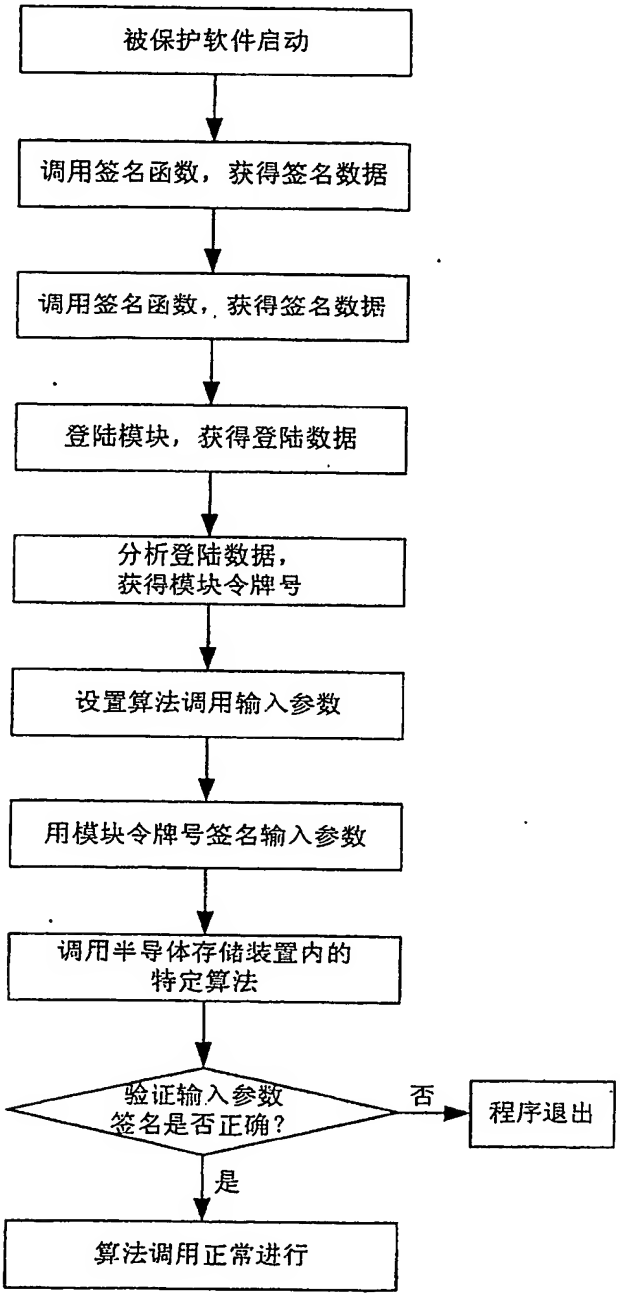

被保护软件启动
调用签名函数，获得签名数据
调用签名函数，获得签名数据
登陆模块，获得登陆数据
分析登陆数据，
获得模块令牌号
设置算法调用输入参数
用模块令牌号签名输入参数
调用半导体存储装置内的
特定算法
验证输入参数
签名是否正确？
否
程序退出
是
算法调用正常进行

图 8

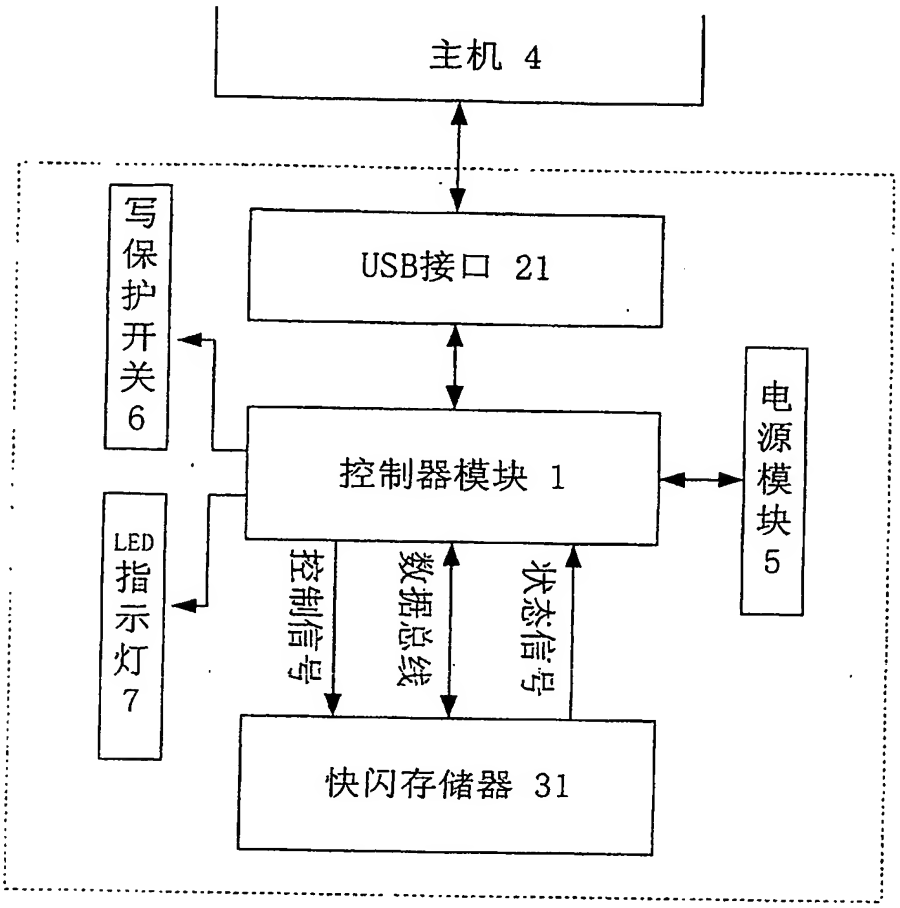

主机 4
USB接口 21
写保护开关 6
控制器模块 1
电源模块 5
LED指示灯 7
控制信号
数据总线
状态信号
快闪存储器 31

图 9

说明书附图

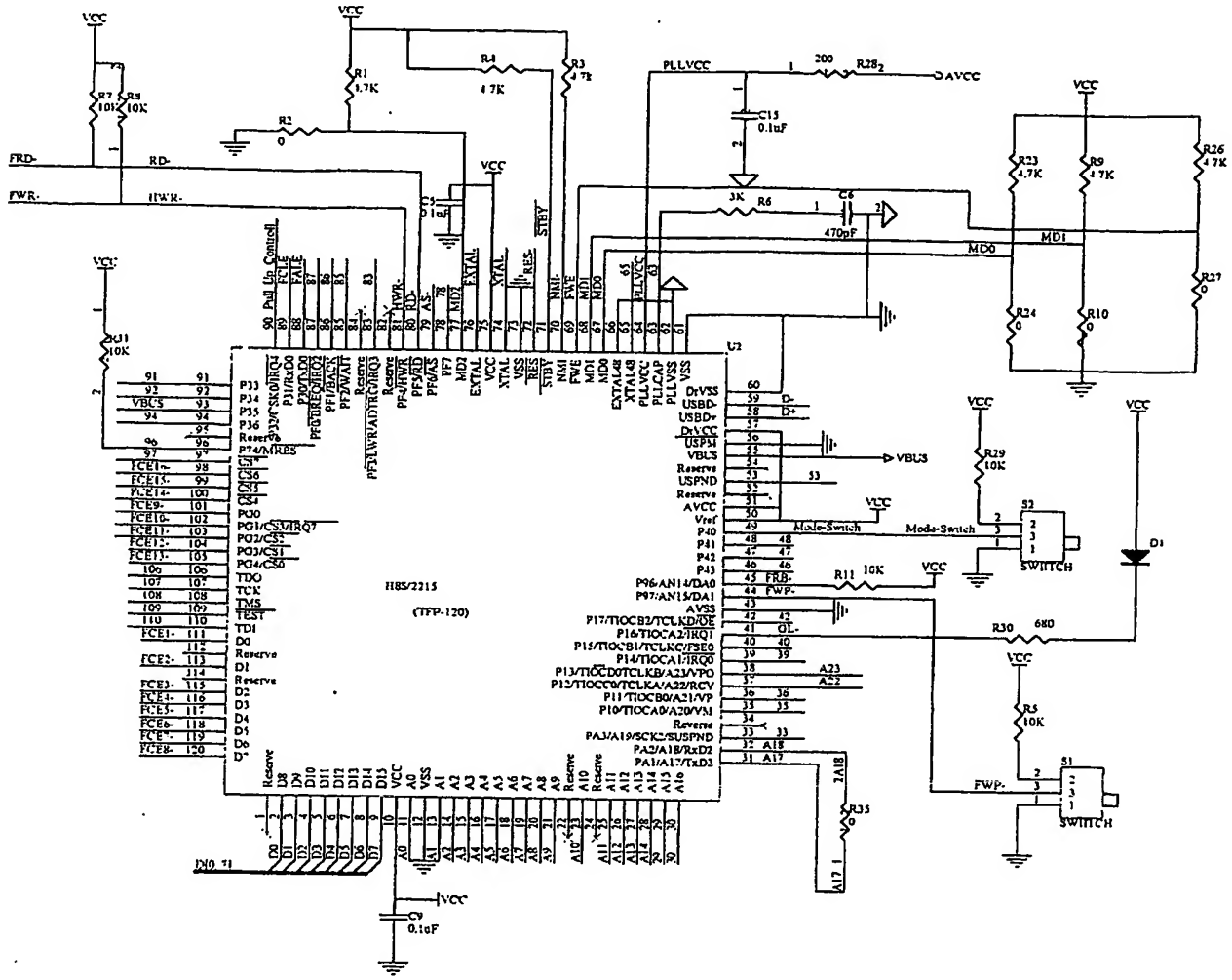

VCC
R1 1.7K
R4 4.7K
R3 4.7K
R2 0
PLLVCC
R28 200
AVCC
C15 0.1uF
R23 4.7K
R9 4.7K
R26 4.7K
FRD-
RD-
FWR-
HWR-
C5 0.1uF
3K R6
C6 470pF
MD1
MD0
R27 0
R24 0
R10 0
R7 10K
R8 10K
R31 10K
U2
H85/2215
(TFP-120)
R29 10K
S2
SWITCH
Mode-Switch
D1
VBUS
R11 10K
FRB-
FWP-
R30 680
R5 10K
S1
SWITCH
R35 0
A23
A22
A18
A17
C9 0.1uF

图 10-A

说明书附图

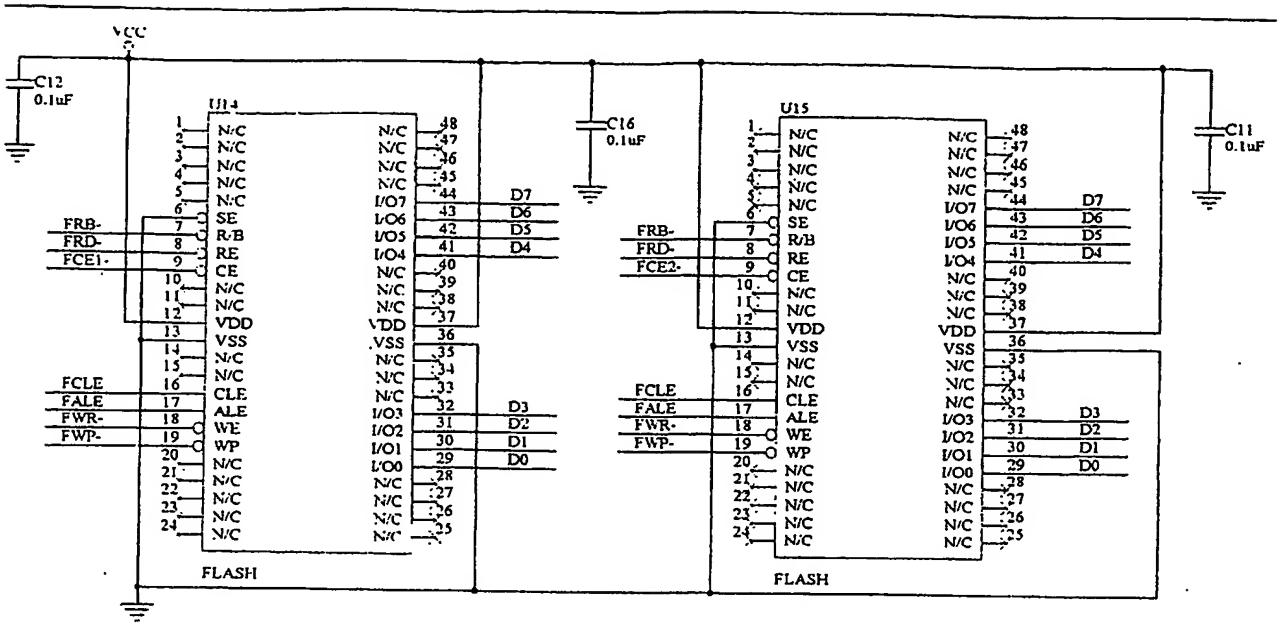


图 10-B

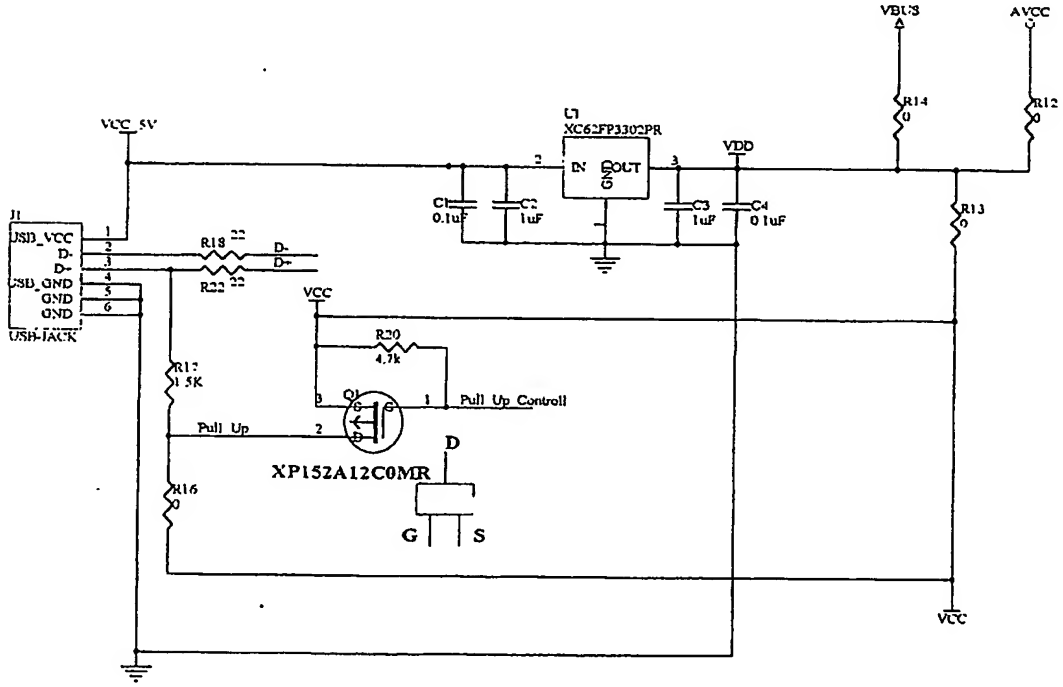


图 10-C